An Anti-Jamming Strategy for Disco Intelligent Reflecting Surfaces Based Fully-Passive Jamming Attacks

Huan Huang*, Hongliang Zhang†, Yi Cai*, A. Lee Swindlehurst‡, and Zhu Han§
* School of Electronic and Information Engineering, Soochow University, Suzhou, China
† School of Electronics, Peking University, Beijing, China
‡ Department of Electrical and Computer Engineering, University of Houston, Houston, USA
§ Center for Pervasive Communications and Computing, University of California, Irvine, USA
Email: hhuang1799@gmail.com, hongliang.zhang92@gmail.com, yicai@ieee.org, swindle@uci.edu, hanzhu22@gmail.com

GLOBECOM 2023 - 2023 IEEE Global Communications Conference | 979-8-3503-1090-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/GLOBECOM54140.2023.10437412

***Abstract*—Emerging intelligent reflecting surfaces (IRSs) significantly improve system performance, while also pose a huge risk for physical layer security. A disco IRS (DIRS), i.e., an illegitimate IRS with random time-varying reflection properties, can be employed by an attacker to actively age the channels of legitimate users (LUs). Such active channel aging (ACA) generated by the DIRS-based fully-passive jammer (FPJ) can be applied to jam multi-user multiple-input single-output (MU-MISO) systems without relying on either jamming power or LU channel state information (CSI). To address the significant threats posed by the DIRS-based FPJ, an anti-jamming strategy is proposed that requires only the statistical characteristics of DIRS-jammed channels instead of their CSI. Statistical characteristics of DIRS-jammed channels are first derived, and then the anti-jamming precoder is given based on the derived statistical characteristics. Numerical results are also presented to evaluate the effectiveness of the proposed anti-jamming precoder against the DIRS-based FPJ.**

***Index Terms*—Physical layer security, intelligent reflecting surface, transmit precoding, jamming suppression.**

I. Introduction

Due to the open communication environment in wireless broadcast and superposition channels, wireless networks are vulnerable to malicious attacks such as jamming (also known as DoS-type attacks) and eavesdropping [1], [2]. Jamming attacks can be launched by an active jammer (AJ), which inflicts intentional jamming/interference to block a communication between the wireless access point (AP) and its legitimate users (LUs). Generally, physical-layer AJs can be divided into the following categories [2]: constant AJs, intermittent AJs, reactive AJs, and adaptive AJs.

Recently, intelligent reflecting surfaces (IRSs), a promising wireless technology for future 6G communications, have been proposed to reflect electromagnetic waves in a controlled manner [3], [4]. Previous works have focused mainly on the introduction of legitimate IRSs to improve certain performance metrics such as energy efficiency (EE) [5], spectrum efficiency (SE) [6], or cell coverage [7]. However, some works have pointed out that illegitimate IRSs can impose a significant impact on wireless networks because the illegitimate IRSs are difficult to detect due to their passive nature [8]. Fortunately, active jamming of the LUs by the illegitimate IRS requires channel state information (CSI) of all LU channels involved. If the illegitimate IRS wants to acquire LU CSI, it needs to estimate the CSI jointly with the legitimate AP and LUs, and thus it is very difficult to implement in practice.

An interesting fully-passive jammer (FPJ) [9], [10] has been proposed to launch jamming attacks on LUs with neither LU CSI nor jamming power, where an illegitimate IRS with random phase shifts, referred to as a "disco" IRS (DIRS), is used to actively age the LUs' channels to cause serious active channel aging (ACA) interference. Classical anti-jamming approaches [11], such as spread spectrum and frequency-hopping techniques, can not be used against this type of FPJ. This is because the source of jamming attacks launched by the FPJ comes from the legitimate AP transmit signals, and therefore always has the same characteristics (such as the carrier frequency) as the transmit signals.

In addition, the jamming attacks from the DIRS-based FPJ, i.e., the ACA interference, can not be mitigated using multi-input multi-output (MIMO) interference cancellation [12]. MIMO interference cancellation is effective only if the information of both the LU and DIRS-jammed channels is known by the legitimate AP [11], [12]. However, the DIRS electromagnetic responses (such as phase shifts and amplitudes) are randomly generated [9], [10]. In summary, there is no effective anti-jamming approach available to counteract the destructive DIRS-based ACA interference imposed by the FPJ.

In this paper, we investigate DIRS-based ACA interference caused by an FPJ and propose an effective anti-jamming strategy. The main contributions are summarized as follows:

- We consider a practical IRS model in which the phase shifts of the DIRS reflecting elements are discrete and the amplitudes are a function of their corresponding phase shifts. Based on this IRS model, we describe the DIRS-based FPJ, which initiates jamming attacks through the DIRS-based ACA interference and requires no additional jamming power or knowledge of the LU CSI.
- To address the significant threats posed by the DIRS-based FPJ, we develop an anti-jamming strategy that re-

This work was supported by the National Key R&D Program of China (2022YFB2903000) and the National Natural Science Foundation of China (62275185, 62250710164), and partially supported by the U.S. National Science Foundation (CNS-2107216, CNS-2128368, CMMI-2222810, ECCS-2030029, CNS-2107182), US Department of Transportation, Toyota, and Amazon (*Corresponding author: Huan Huang*).

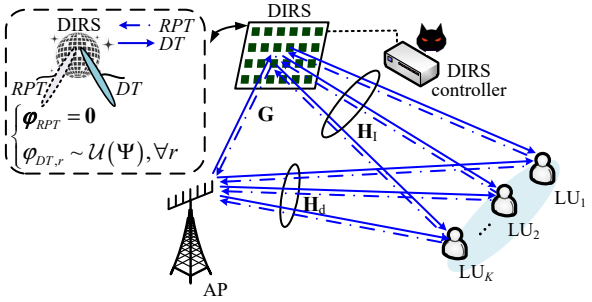

Fig. 1. Illustration of fully passive jamming (FPJ) implemented by disco intelligent reflecting surface (DIRS) based active channel aging in an MU-MISO system. RPT: reverse pilot transmission; DT: data transmission.

quires only the statistical characteristic of DIRS-jammed channels and avoids requiring their instantaneous CSI, which is impractical to obtain. We first derive the statistical characteristic of the DIRS-jammed channels, and then prove that the developed anti-jamming precoder achieves the maximum signal-to-jamming-plus-noise ratio (SJNR).

The rest is organized as follows. In Section II, we consider a practical IRS model and describe the general mode of the DIRS-based FPJ. Then, we define the SJNR optimization metric and present the channel model. In Section III, we first derive a statistical characteristic of the DIRS-jammed channels. Then, we develop an anti-jamming precoder based on the derived statistical characteristic and prove that this precoder can achieve the maximum SJNR. Simulation results are provided in Section IV to show the effectiveness of the proposed anti-jamming precoder against the DIRS-based FPJ. Finally, the main conclusions are given in Section V.

We employ bold capital type for a matrix, e.g., $\boldsymbol{\Phi}_{DT}$, small bold type for a vector, e.g., $\boldsymbol{w}_{RPT,k}$, and italic type for a scalar, e.g., K. The superscripts $(\cdot)^H$ and $(\cdot)^{-1}$ represent the Hermitian transpose and the inverse. The symbols $|\cdot|$ and $\|\cdot\|$ denote the absolute value and the Frobenius norm.

II. System Statement

A. Disco-IRS-Based Fully-Passive Jammer

Fig. 1 diagrammatically demonstrates an MU-MISO system jammed by the DIRS-based FPJ. Specifically, the legitimate AP has N_A antennas and communicates with K single-antenna LUs denoted by $\mathrm{LU}_1, \mathrm{LU}_2, \cdots, \mathrm{LU}_K$. A DIRS consisting of N_D reflecting elements with one-bit quantized phase is placed relatively close to the AP[1] to jam the LUs.

In an MU-MISO system, the channel coherence time consists of two phases, i.e., a *reverse pilot transmission (RPT)* phase and a *data transmission (DT)* phase. In general, the wireless channels in an MU-MISO system are assumed to remain unchanged during the channel coherence time. Therefore, the CSI is estimated during the *RPT* phase, and the downlink precoding is then designed based on the obtained CSI and used to transmit signals to the LUs during the *DT* phase. However, the work in [9], [10] has shown that the DIRS can be used to actively age the channels, i.e., create rapidly changing wireless channels within the channel coherence time. The DIRS-based ACA differs from channel aging (CA) in traditional MU-MISO systems [13]. In fact, CA is CSI inaccuracy due to time variation of channels and computation delays, and it can not be actively introduced and controlled.

1) Data Transmission: During the *DT* phase, the signal received at LU_k is given by

$$\begin{aligned} y_k &= \boldsymbol{h}_{DT,k}^H \sum_{u=1}^{K} \boldsymbol{w}_{RPT,u} s_u + n_k \\ &= \left(\boldsymbol{h}_{\mathrm{I},k}^H \boldsymbol{\Phi}_{DT} \mathbf{G} + \boldsymbol{h}_{\mathrm{d},k}^H\right) \sum_{u=1}^{K} \boldsymbol{w}_{RPT,u} s_u + n_k, \end{aligned} \tag{1}$$

where the transmitted signal $s_u \in \mathbb{C}$ satisfies $\mathbb{E}\left[s_u s_u^H\right] = 1$. In addition, $\boldsymbol{h}_{DT,k}^H \in \mathbb{C}^{1\times N_\mathrm{A}}$ represents the combined channel between the legitimate AP and LU_k, $\boldsymbol{h}_{\mathrm{I},k} \in \mathbb{C}^{N_\mathrm{D}\times 1}$ represents the channel between the DIRS and LU_k, $\mathbf{G} = \left[\boldsymbol{g}_1, \cdots, \boldsymbol{g}_{N_\mathrm{A}}\right] \in \mathbb{C}^{N_\mathrm{D}\times N_\mathrm{A}}$ represents the channel between the legitimate AP and the DIRS, and $\boldsymbol{h}_{\mathrm{d},k} \in \mathbb{C}^{N_\mathrm{A}\times 1}$ represents the direct channel between the legitimate AP and LU_k. Furthermore, n_k denotes additive white Gaussian noise (AWGN) with zero mean and variance σ^2, i.e., $n_k \sim \mathcal{CN}\left(0, \sigma^2\right)$. For ease of presentation, the overall DIRS-LU channel $\mathbf{H}_\mathrm{I}$ and the overall LU direct channel $\mathbf{H}_\mathrm{d}$ are denoted as $\mathbf{H}_\mathrm{I} = [\boldsymbol{h}_{\mathrm{I},1}, \cdots, \boldsymbol{h}_{\mathrm{I},K}]$ and $\mathbf{H}_\mathrm{d} = [\boldsymbol{h}_{\mathrm{d},1}, \cdots, \boldsymbol{h}_{\mathrm{d},K}]$, respectively. Furthermore, the DIRS-jammed channel $\mathbf{H}_\mathrm{D}^{DT}$ is denoted as $\mathbf{H}_\mathrm{D}^{DT} = \mathbf{H}_\mathrm{I}^H \boldsymbol{\Phi}_{DT} \mathbf{G} = \left[\boldsymbol{h}_{\mathrm{D},1}^{DT}, \cdots, \boldsymbol{h}_{\mathrm{D},K}^{DT}\right]$.

In (1), $\boldsymbol{\Phi}_{DT} = \mathrm{diag}(\boldsymbol{\varphi}_{DT}(t)) \in \mathbb{C}^{N_\mathrm{D}\times N_\mathrm{D}}$ denotes the passive beamformer of the DIRS during the DT phase. The reflecting vector $\boldsymbol{\varphi}_{DT}(t)$ is randomly generated and given by $\boldsymbol{\varphi}_{DT}(t) = \left[\beta_{DT,1}(t) e^{j\varphi_{DT,1}(t)}, \cdots, \beta_{DT,N_\mathrm{D}}(t) e^{j\varphi_{N_\mathrm{D}}(t)}\right]$, where $\beta_{DT,r}(t)$ and $\varphi_{DT,r}(t)$ $(r = 1, \cdots, N_\mathrm{D})$ denote the amplitude and phase shift of the r-th DIRS reflecting element, respectively. An IRS is an ultra-thin surface inlaid with multiple sub-wavelength reflecting elements whose electromagnetic responses are controlled by programmable PIN diodes [4]. Based on the ON/OFF behavior of PIN diodes, only a few discrete phase shifts are generated by an IRS.

For a DIRS with b-bit quantized phase shifts, let $\Psi = \{\theta_1, \cdots, \theta_{2^b}\}$ represent the set of discrete phase shift values. Assume that the DIRS phase shifts are randomly selected from Ψ, i.e., $\varphi_{DT,r}(t) \sim \mathcal{R}(\Psi)$. The gain values $\beta_{DT,r}(t)$ are a function of $\varphi_{DT,r}(t)$ [3], which we express as $\beta_{DT,r}(t) = \mathcal{F}\left(\varphi_{DT,r}(t)\right)$. We denote the set of all possible amplitude values as $\Omega = \mathcal{F}(\Psi) = \{\kappa_1, \cdots, \kappa_{2^b}\}$. Note that, in practice, the independent DIRS controller does not have sufficient computing power to generate complex distributions for the DIRS reflecting vector $\boldsymbol{\varphi}_{DT}(t)$ [9], [10]. Therefore, we assume that the illegitimate DIRS jams the MU-MISO system with reflecting phase shifts that follow a uniform distribution, i.e.,

[1]Many existing performance-enhancing IRS-based systems assume that legitimate IRSs are placed close to the users to maximize system performance [5], [6], [7]. However, here we make the more robust assumption that the DIRS controller has no LU information [9], [10]. Therefore, the DIRS is placed relatively close to the AP to maximize the impact of the DIRS.

$\varphi_{DT,r}(t) \sim \mathcal{U}(\Psi)$.

2) Reverse Pilot Transmission: To optimize the multi-user active beamforming $\mathbf{W}_{RPT} = [\boldsymbol{w}_{RPT,1}, \cdots, \boldsymbol{w}_{RPT,K}] \in \mathbb{C}^{N_\mathrm{A} \times K}$, the legitimate AP needs to obtain the LUs' CSI using pilot-based channel estimation after the RPT phase. Specifically, the LUs send pilot symbols to the legitimate AP, and the AP then estimates the channel using, for example, a traditional solution such as the least squares (LS) algorithm.

During the RPT phase, the DIRS reflecting vector is denoted by $\boldsymbol{\varphi}_{RPT}(t)$. Similar to [10], the DIRS remains silent during the RPT phase, i.e., $\boldsymbol{\varphi}_{RPT}(t) = \mathbf{0}$, which means that the wireless signals are perfectly absorbed by the illegitimate DIRS. Consequently, the overall multiuser channel estimated by the legitimate AP is written as

$$\mathbf{H}_{RPT}^H = [\boldsymbol{h}_{RPT,1}, \cdots, \boldsymbol{h}_{RPT,K}]^H = \mathbf{H}_\mathrm{d}^H. \tag{2}$$

Generally, the aim of the multi-user active beamforming optimization is to maximize the signal power and minimize the interference leakage. Based on the CSI obtained for $\mathbf{H}_{RPT}$, a widely-used approach is the zero-forcing beamforming (ZFBF) [14], which results in zero interference leakage. Specifically, $\mathbf{W}_{RPT}$ calculated with the ZFBF algorithm is given by

$$\mathbf{W}_{RPT} = \mathbf{H}_{RPT}\left(\mathbf{H}_{RPT}^H \mathbf{H}_{RPT}\right)^{-1} \mathbf{P}^{\frac{1}{2}} = [\boldsymbol{w}_{RPT,1}, \cdots, \boldsymbol{w}_{RPT,K}], \tag{3}$$

where $\|\boldsymbol{w}_{RPT,k}\| = \sqrt{p_k}$ and p_k represents the transmit power of LU_k. The total transmit power P_0 at the legitimate AP satisfies the constraint that $\sum_{k=1}^{K} p_k \le P_0$. For simplicity, we assume that $p_k = \frac{P_0}{K}, \forall k$.

3) Active channel Aging: In a traditional MU-MISO system, a wireless channel is assumed to be essentially invariant during its coherence time. Each coherence time includes an RPT phase and a much longer DT phase, and thus the CSI obtained in the RPT phase is assumed to be the same as in the DT phase.

However, an IRS offers the ability to actively age the channel [9], [10] and produces a situation where the CSI obtained in the RPT phase is different from that in the DT phase. As a result, serious DIRS-based ACA interference is introduced. The SJNR for LU_k quantifies the DIRS-based ACA interference, and based on (1) is given by [15], [16]:

$$\eta_k = \frac{\mathbb{E}\left[\left|\boldsymbol{h}_{DT,k}^H \boldsymbol{w}_{RPT,k}\right|^2\right]}{\sum\limits_{u \ne k} \mathbb{E}\left[\left|\boldsymbol{h}_{DT,u}^H \boldsymbol{w}_{RPT,k}\right|^2\right] + \sigma^2}. \tag{4}$$

B. Channel Model

Since the DIRS is deployed relatively close to the legitimate AP, the AP-DIRS channel $\mathbf{G}$ is assumed to follow Rician fading [17]. Meanwhile, the overall DIRS-LU channel $\mathbf{H}_\mathrm{I}$ and the overall LU direct channel $\mathbf{H}_\mathrm{d}$ are assumed to follow Rayleigh fading [17]. Mathematically, $\mathbf{G}$ is modelled as

$$\mathbf{G} = \sqrt{\mathscr{L}_\mathrm{G}}\left(\sqrt{\frac{\varepsilon}{1+\varepsilon}}\mathbf{G}^{\mathrm{LOS}} + \sqrt{\frac{1}{1+\varepsilon}}\mathbf{G}^{\mathrm{NLOS}}\right), \tag{5}$$

where $\mathscr{L}_\mathrm{G}$ represents the large-scale channel fading for $\mathbf{G}$, ε is the Rician factor, and $\mathbf{G}^{\mathrm{LOS}}$ and $\mathbf{G}^{\mathrm{NLOS}}$ denote the line-of-sight (LOS) and non-line-of-sight (NLOS) component of $\mathbf{G}$. More specifically, $\mathbf{G}^{\mathrm{NLOS}}$ has i.i.d. elements given by $\left[\mathbf{G}^{\mathrm{NLOS}}\right]_{r,n} \sim \mathcal{CN}(0,1)$. Moreover, the DIRS is deployed close to the legitimate AP, and thus the element $\left[\mathbf{G}^{\mathrm{LOS}}\right]_{r,n}$ is characterized by the near-field model [18] as follows:

$$\left[\mathbf{G}^{\mathrm{LOS}}\right]_{r,n} = e^{-j\frac{2\pi}{\lambda}(D_n^r - D_n)}, \tag{6}$$

where λ represents the wavelength of the transmit signals, and D_n^r and D_n denote the distance between the n-th antenna and the r-th DIRS reflecting element, and the distance between the n-th antenna and the centre (origin) of the DIRS, respectively. We assume that both the distance between adjacent antennas and the distance between adjacent DIRS reflecting elements are $d = \lambda/2$.

The channels $\mathbf{H}_\mathrm{I}$ and $\mathbf{H}_\mathrm{d}$ are mathematically modelled as

$$\mathbf{H}_\mathrm{I} = \widehat{\mathbf{H}}_\mathrm{I}\mathbf{D}_\mathrm{I}^{1/2} = \left[\sqrt{\mathscr{L}_{\mathrm{I},1}}\widehat{\boldsymbol{h}}_{\mathrm{I},1}, \cdots, \sqrt{\mathscr{L}_{\mathrm{I},K}}\widehat{\boldsymbol{h}}_{\mathrm{I},K}\right], \tag{7}$$

$$\mathbf{H}_\mathrm{d} = \widehat{\mathbf{H}}_\mathrm{d}\mathbf{D}_\mathrm{d}^{1/2} = \left[\sqrt{\mathscr{L}_{\mathrm{d},1}}\widehat{\boldsymbol{h}}_{\mathrm{d},1}, \cdots, \sqrt{\mathscr{L}_{\mathrm{d},K}}\widehat{\boldsymbol{h}}_{\mathrm{d},K}\right], \tag{8}$$

where the elements of the $K \times K$ diagonal matrices $\mathbf{D}_\mathrm{I} = \mathrm{diag}(\mathscr{L}_{\mathrm{I},1}, \cdots, \mathscr{L}_{\mathrm{I},K})$ and $\mathbf{D}_\mathrm{d} = \mathrm{diag}(\mathscr{L}_{\mathrm{d},1}, \cdots, \mathscr{L}_{\mathrm{d},K})$ represent the large-scale channel fading. Moreover, the i.d.d. elements of $\widehat{\mathbf{H}}_\mathrm{I}$ and $\widehat{\mathbf{H}}_\mathrm{d}$ are defined as $[\widehat{\mathbf{H}}_\mathrm{I}]_{r,k}, [\widehat{\mathbf{H}}_\mathrm{d}]_{n,k} \sim \mathcal{CN}(0,1)$, $r = 1, \cdots, N_\mathrm{D}$, $n = 1, \cdots, N_\mathrm{A}$, and $k = 1, \cdots, K$.

III. An Anti-Jamming Strategy for Disco-IRS-Based Fully-Passive Jammers

As mentioned in Section I, it is unrealistic for the legitimate AP to have the knowledge of the DIRS-jammed channel $\mathbf{H}_\mathrm{D}^{DT}$. In order to develop an anti-jamming precoder for the DIRS-based FPJ presented in Section II, we derive the following statistical characteristic of $\mathbf{H}_\mathrm{D}^{DT}$, i.e., Proposition 1.

Proposition 1: The i.d.d. elements of $\mathbf{H}_\mathrm{D}^{DT}$ converge in distribution to $\mathcal{CN}\left(0, \mathscr{L}_\mathrm{G}\mathscr{L}_{\mathrm{I},k}N_\mathrm{D}\delta^2\right)$ as $N_\mathrm{D} \to \infty$, i.e.,

$$\left[\mathbf{H}_\mathrm{D}^{DT}\right]_{k,n} \xrightarrow{\mathrm{d}} \mathcal{CN}\left(0, \mathscr{L}_\mathrm{G}\mathscr{L}_{\mathrm{I},k}N_\mathrm{D}\delta^2\right), \forall k, n, \tag{9}$$

where $\delta^2 = \frac{\sum_{i=1}^{2^b}\kappa_i^2}{2^b}$.

Proof: See Appendix A. ∎

It is worth noting that the DIRS-based FPJ is deployed in practice with a large number of reflecting elements, i.e., $N_\mathrm{D} \gg 1$. According to the previous work [10], the DIRS must be equipped with a massive number of elements in order to launch significant jamming attacks since the large-scale channel fading in the DIRS-jammed channel $\mathbf{H}_\mathrm{D}^{DT}$ is much more severe than that in the overall LU direct channel $\mathbf{H}_\mathrm{d}$.

According to Proposition 1, the legitimate AP can use the anti-jamming precoder given in Theorem 1 to maximize the SJNR expressed by (4).

Theorem 1: The optimal precoder for LU_k to mitigate the jamming attacks launched by the DIRS-based FPJ, i.e., to maximize the SJNR η_k, is given by

$$\boldsymbol{w}_{\mathrm{Anti},k} \propto \max.\mathrm{eigenvector}(\mathbf{A}_k), \tag{10}$$

where

$$\mathbf{A}_k = \left(\boldsymbol{h}_{\mathrm{d},k}\boldsymbol{h}_{\mathrm{d},k}^H + \mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},k}N_{\mathrm{D}}\alpha\mathbf{I}_{N_{\mathrm{A}}}\right) \times \left(\widetilde{\mathbf{H}}_{\mathrm{d},k}\widetilde{\mathbf{H}}_{\mathrm{d},k}^H + \left(\frac{\sigma^2}{p_k} + \sum_{u\neq k}\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},u}N_{\mathrm{D}}\alpha\right)\mathbf{I}_{N_{\mathrm{A}}}\right)^{-1}, \quad (11)$$

$\max.\text{eigenvector}\left(\mathbf{A}_k\right)$ denotes the eigenvector of $\mathbf{A}_k$ associated with the largest eigenvalue, and $\widetilde{\mathbf{H}}_{\mathrm{d},k} = [\boldsymbol{h}_{\mathrm{d},1}, \cdots, \boldsymbol{h}_{\mathrm{d},k-1}, \boldsymbol{h}_{\mathrm{d},k+1}, \cdots, \boldsymbol{h}_{\mathrm{d},K}]$.

Proof: In (4), the overall LU direct channel $\mathbf{H}_{\mathrm{d}}$ and the multi-user active beamforming $\mathbf{W}_{RPT}$ are fixed during the channel coherence time. Consequently, the SJNR at LU_k in (4) reduces to

$$\eta_k = \frac{\left|\boldsymbol{h}_{\mathrm{d},k}^H\boldsymbol{w}_{RPT,k}\right|^2 + \boldsymbol{w}_{RPT,k}^H\mathbb{E}\left[\boldsymbol{h}_{\mathrm{D},k}^{DT}(\boldsymbol{h}_{\mathrm{D},k}^{DT})^H\right]\boldsymbol{w}_{RPT,k}}{\sum\limits_{u\neq k}\left(\left|\boldsymbol{h}_{\mathrm{d},u}^H\boldsymbol{w}_{RPT,k}\right|^2 + \boldsymbol{w}_{RPT,k}^H\mathbb{E}\left[\boldsymbol{h}_{\mathrm{D},u}^{DT}(\boldsymbol{h}_{\mathrm{D},u}^{DT})^H\right]\boldsymbol{w}_{RPT,k}\right) + \sigma^2}. \quad (12)$$

According to (12) and Proposition 1, the following equation can be generated, i.e.,

$$\eta_k = \frac{\boldsymbol{w}_{RPT,k}^H\widehat{\mathbf{H}}_{DT,k}\boldsymbol{w}_{RPT,k}}{\boldsymbol{w}_{RPT,k}^H\widehat{\widetilde{\mathbf{H}}}_{DT,k}\boldsymbol{w}_{RPT,k}}, \quad (13)$$

where $\widehat{\mathbf{H}}_{DT,k} = \boldsymbol{h}_{\mathrm{d},k}\boldsymbol{h}_{\mathrm{d},k}^H + \left(\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},k}N_{\mathrm{D}}\delta^2\right)\mathbf{I}_{N_{\mathrm{A}}}$ and $\widehat{\widetilde{\mathbf{H}}}_{DT,k} = \widetilde{\mathbf{H}}_{\mathrm{d},k}\widetilde{\mathbf{H}}_{\mathrm{d},k}^H + \left(\frac{\sigma^2}{p_k} + \sum_{u\neq k}\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},u}N_{\mathrm{D}}\delta^2\right)\mathbf{I}_{N_{\mathrm{A}}}$.

Using the Rayleigh-Ritz quotient [15] we have

$$\eta_k \leq \lambda_{\max}\left(\widehat{\mathbf{H}}_{DT,k}, \widehat{\widetilde{\mathbf{H}}}_{DT,k}\right). \quad (14)$$

Based on (14), the anti-jamming precoder for LU_k that maximizes the SJNR η_k is given by

$$\boldsymbol{w}_{\mathrm{Anti},k} = \sqrt{p_k}\frac{\max.\text{eigenvector}\left(\mathbf{A}_k\right)}{\|\max.\text{eigenvector}\left(\mathbf{A}_k\right)\|}. \quad (15)$$

■

As a result, the legitimate AP can exploit the anti-jamming precoder in Theorem 1 to mitigate the jamming attacks launched by the DIRS-based FPJ [9], [10].

IV. Simulation Results and Discussion

In this section, we present numerical results to evaluate the effectiveness of the proposed anti-jamming precoder against the DIRS-based FPJ [9], [10]. We consider an MU-MISO system where the legitimate AP is equipped with 16 antennas and communicates with eight LUs, i.e., $N_{\mathrm{A}} = 16$ and $K = 8$. Meanwhile, the MU-MISO system is jammed by the DIRS-based FPJ described in Section II-A, where the DIRS has (32×32) reflecting elements, i.e., $N_{\mathrm{D}} = 1024$. We further consider a one-bit DIRS that is easy to implement in practice, where $\Psi = \left\{\frac{\pi}{9}, \frac{6\pi}{5}\right\}$ and $\Omega = \mathcal{F}(\Psi) = \{0.8, 1\}$ [3]. In other words, the r-th element of the reflecting vector $\boldsymbol{\varphi}_{DT}(t)$ satisfies $\beta_{DT,r}(t)e^{j\varphi_{DT,r}(t)} \in \left\{0.8e^{j\frac{\pi}{9}}, e^{j\frac{6\pi}{5}}\right\}$. Consequently, the variance in (9) is calculated as $\delta^2 = 0.82$.

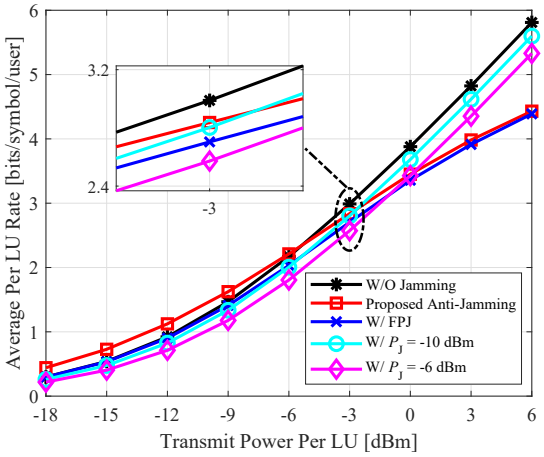

Fig. 2. Average rate of each legitimate user (LU) vs. transmit power of each LU for different benchmarks.

The legitimate AP and the DIRS are located at (0m, 0m, 2m) and (2m, 0m, 2m), respectively. The LUs are randomly distributed in a circular region centred at (0m, 180m, 0m) with a radius of 10m. According to the 3GPP propagation model [19], the propagation parameters of the wireless channels modelled in Section II-B are described as follows: $\mathscr{L}_{\mathrm{G}} = 35.6+22\log_{10}(d_i)$ and $\mathscr{L}_k = \mathscr{L}_{\mathrm{I},k} = 32.6+36.7\log_{10}(d_i)$, where $d_i \in \{d_{\mathrm{G}}, d_{\mathrm{I},k}, d_{\mathrm{d},k}\}$ is the propagation distance. Moreover, the AWGN variance is $\sigma^2 = -170 + 10\log_{10}(BW)$ dBm, where the transmission bandwidth is $BW = 180$ kHz.

Herein, we illustrate the average rate per LU[2] achieved by the following benchmarks: the rate resulting from an MU-MISO system without jamming attacks (W/O Jamming) [14]; the rate resulting from an MU-MISO system using the proposed anti-jamming precoder presented in Section III (Proposed Anti-Jamming); the rate resulting from an MU-MISO system under the DIRS-based fully-passive jamming attacks [9], [10] (W/FPJ); and the rate resulting from an MU-MISO system under active jamming attacks. In the latter case, two cases are considered with an AJ located at (2m, 0m, 2m) broadcasting jamming signals with -10 dBm jamming power (W/ $P_{\mathrm{J}} = -10$ dBm) and -6 dBm jamming power (W/ $P_{\mathrm{J}} = -6$ dBm).

Fig. 2 illustrates the relationship between the average rate per LU and the transmit power per LU. Compared to the average rate per LU obtained W/O Jamming, the results for the proposed anti-jamming precoder are better in the low power domain. This is because the anti-jamming precoder given in Theorem 1 can (to some extent) exploit the signals transmitted in the DIRS-jammed channel to improve the SJNR of each LU. The work in [14] showed that maximising the LU signal power in the low power domain can achieve near-optimal performance. In practice, many MU-MISO systems

[2]The rate per LU is defined as $\frac{1}{K}\sum\limits_{k=1}^{K}\log_2\left(1 + \frac{\left|\boldsymbol{h}_{DT,k}^H\boldsymbol{w}_{RPT,k}\right|^2}{\sum\limits_{u\neq k}\left|\boldsymbol{h}_{DT,u}^H\boldsymbol{w}_{RPT,k}\right|^2 + \sigma^2}\right)$.

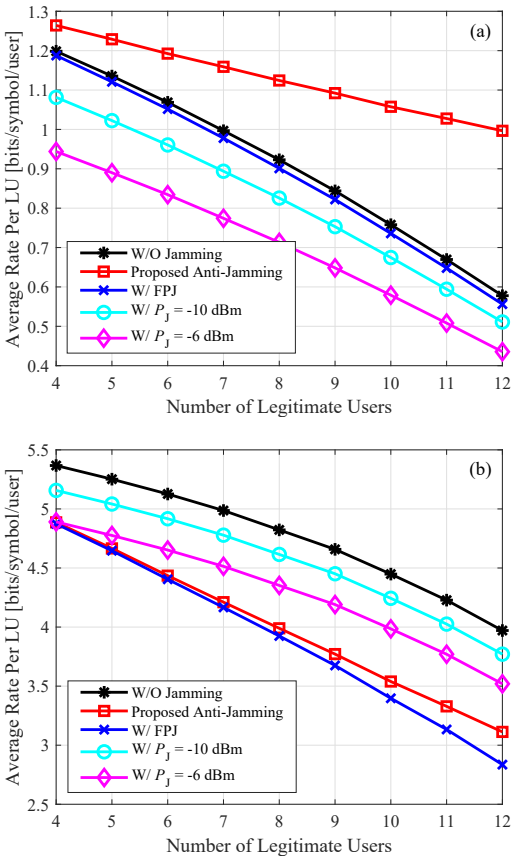

Fig. 3. Number of legitimate users (LUs) vs. average rate per LU for (a) -12 dBm and (b) 3 dBm transmit power per LU.

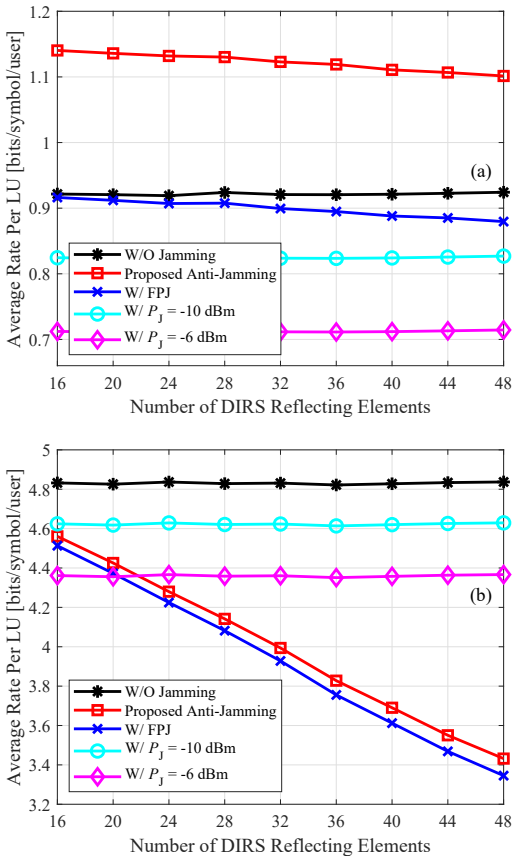

Fig. 4. Number of DIRS reflecting elements vs. average rate per LU for (a) -12 dBm and (b) 3 dBm transmit power per LU.

using low-order modulations, such as quadrature phase shift keying (QPSK), work in the low transmit power domain.

On the other hand, inter-user interference (IUI) dominates the noise for high transmit power [14]. Although the proposed anti-jamming precoder can to some extent exploit the signals transmitted in the DIRS-jammed channel, it also amplifies the interference due to the leakage from the DIRS-jammed channel. As a result, the average rate per LU resulting from the anti-jamming precoder is weaker than that for W/O Jamming. Compared to the rates archived by W/FPJ, the results obtained for the proposed anti-jamming algorithm are always better. For example, when the transmit power per LU is -3 dBm, the jamming impact of the DIRS-based FPJ is more serious than that of AJ with -10 dBm jamming power. However, using the proposed anti-jamming precoder, the DIRS-based jamming attacks are mitigated, and are even weaker than the jamming attacks launched by the AJ with -10 dBm jamming power.

Fig. 3 shows the average rate per LU versus the number of LUs. The results for low transmit power ($p_k = -12$ dBm) and high transmit power ($p_k = 3$ dBm) are depicted in Fig. 3 (a) and Fig. 3 (b), respectively. The rates resulting from all benchmarks decrease with the number of LUs due to the increase in IUI and the decrease in available MIMO gain. As mentioned above, the average rate per LU resulting from the anti-jamming precoder is higher than that resulting from W/O Jamming in the low power domain. From Fig. 3 (a), one can see that the gap in average rate between the Proposed Anti-Jamming and W/FPJ increases with the number of LUs. As the number of LUs increases, the gain generated from the jammed channel becomes more significant due to the anti-jamming precoder.

In addition, the difference between the rate of W/O Jamming and the rate obtained with active jamming attacks gradually decreases as the number of LUs increases. This is due to the fact that the increase in IUI detracts from the rates, while at the same time weakening the impact of AJ. However, a unique property of the DIRS-based FPJ [9], [10] is that its jamming impact does not decrease as the number of LUs increases, but actually becomes more severe. Fortunately, as can be seen from Fig. 3, the jamming mitigation generated by the anti-jamming precoder becomes more effective as the number of LUs increases.

Fig 4 displays the average rate per LU versus the number of DIRS reflecting elements for low transmit power ($p_k = -12$ dBm) and high transmit power ($p_k = 3$ dBm), respectively. Although the jamming impact of the DIRS-based FPJ becomes more severe as the number of DIRS reflecting elements increases, the proposed anti-jamming precoder always achieves

higher average rates compared to the results of W/FPJ at both low and high transmit power.

V. Conclusions

In this paper, to address the significant threats posed by DIRS-based FPJ, a novel anti-jamming precoder has been developed that can be implemented using only the statistical characteristics of the DIRS-jammed channel instead of the instantaneous CSI. We have showed that the elements of the DIRS-jammed channel follow a complex Gaussian distribution with zero mean and variance $\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},k}N_{\mathrm{D}}\delta^2$. Based on this derived statistical characteristic, we have developed an anti-jamming precoder that can achieve the maximum SJNR. In particular, for an MU-MISO system operating with low power, the proposed anti-jamming precoder causes the DIRS-based FPJ to not only fail to jam the LUs, it actually improves the SJNRs of the LUs due to the additional DIRS-jammed channel it provides.

Appendix A
Proof of Proposition 1

The element $\left[\mathbf{H}_{\mathrm{D}}^{DT}\right]_{k,n}$ can be written as

$$\begin{aligned}\left[\mathbf{H}_{\mathrm{D}}^{DT}\right]_{k,n} =& \sqrt{\frac{\varepsilon\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},k}N_{\mathrm{D}}}{1+\varepsilon}}\left(\frac{\sum_{r=1}^{N_{\mathrm{D}}}\left[\widehat{\boldsymbol{h}}_{\mathrm{I},k}\right]_r\beta_{DT,r}(t)e^{j\varphi_{DT,r}(t)}}{\sqrt{N_{\mathrm{D}}}},\right.\\ &\left.\times e^{-j\frac{2\pi}{\lambda}(D_n^r-D_n)}\right)+\sqrt{\frac{\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},k}N_{\mathrm{D}}}{1+\varepsilon}}\left(\frac{\sum_{r=1}^{N_{\mathrm{D}}}\left[\widehat{\boldsymbol{h}}_{\mathrm{I},k}\right]_r}{\sqrt{N_{\mathrm{D}}}}\right.\\ &\left.\times\beta_{DT,r}(t)e^{j\varphi_{DT,r}(t)}\left[\mathbf{G}^{\mathrm{NLOS}}\right]_{r,n}\right), \qquad (16)\end{aligned}$$

where $\left[\widehat{\boldsymbol{h}}_{\mathrm{I},k}\right]_r$ represents the r-th elements of $\widehat{\boldsymbol{h}}_{\mathrm{I},k}$. Conditioned on the fact that the variables $\mathbf{H}_{\mathrm{I}}$, $\boldsymbol{\varphi}_{DT}(t)$, and $\mathbf{G}$ are independent, we have the following expectations:

$$\mathbb{E}\left[a_r\right]=\mathbb{E}\left[\left[\widehat{\boldsymbol{h}}_{\mathrm{I},k}\right]_r\beta_{DT,r}(t)e^{j\varphi_{DT,r}(t)}e^{-j\frac{2\pi}{\lambda}(D_n^r-D_n)}\right]=0, \quad (17)$$

$$\mathbb{E}\left[b_r\right]=\mathbb{E}\left[\left[\widehat{\boldsymbol{h}}_{\mathrm{I},k}\right]_r\beta_{DT,r}(t)e^{j\varphi_{DT,r}(t)}\left[\mathbf{G}^{\mathrm{NLOS}}\right]_{r,n}\right]=0, \quad (18)$$

where $r=1,2,\cdots,N_{\mathrm{D}}$. Furthermore, the variances of a_r and b_r are given by

$$\mathrm{Var}\left[a_r\right]=\mathrm{Var}\left[b_r\right]=\frac{\sum_{i=1}^{2^b}\kappa_i^2}{2^b}=\delta^2, r=1,2,\cdots,N_{\mathrm{D}}. \quad (19)$$

According the central limit theorem, the random variables $\sum_{r=1}^{N_{\mathrm{D}}}\frac{a_r}{\sqrt{N_{\mathrm{D}}}}$ and $\sum_{r=1}^{N_{\mathrm{D}}}\frac{b_r}{\sqrt{N_{\mathrm{D}}}}$ converge in distribution to a normal $\mathcal{CN}\left(0,\delta^2\right)$ as $N_{\mathrm{D}}\to\infty$. Consequently, we have that

$$\left[\mathbf{H}_{\mathrm{D}}^{DT}\right]_{k,n}\xrightarrow{\mathrm{d}}\mathcal{CN}\left(0,\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},k}N_{\mathrm{D}}\delta^2\right). \quad (20)$$

References

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Spet. 2016.

[3] H. Zhang, S. Zeng, B. Di, Y. Tan, M. D. Renzo, M. Debbah, Z. Han, H. V. Poor, and L. Song, "Intelligent omni-surfaces for full-dimensional wireless communications: Principles, technology, and implementation," *IEEE Commun. Mag.*, vol. 60, no. 2, pp. 39–45, Feb. 2022.

[4] T. Cui, M. Qi, X. Wan, J. Zhao, and Q. Cheng, "Coding metamaterials, digital metamaterials and programmable metamaterials," *Light-Sci. Appl.*, vol. 3, e218, Oct. 2014.

[5] H. Huang, Y. Zhang, H. Zhang, Z. Zhao, C. Zhang, and Z. Han, "Multi-IRS-aided millimeter-wave multi-user MISO systems for power minimization using generalized Benders decomposition," *IEEE Trans. Wireless Commun.*, early access, Mar. 2023, doi: 10.1109/TWC.2023.3257053.

[6] H. Huang, C. Zhang, Y. Zhang, B. Ning, H. Gao, S. Fu, K. Qiu, and Z. Han, "Two-timescale-based beam training for RIS-aided millimeter-wave multi-user MISO systems," *IEEE Trans. Veh. Technol.*, early access, Apr. 2023, doi: 10.1109/TVT.2023.3269153.

[7] S. Zeng, H. Zhang, B. Di, Z. Han, and L. Song, "Reconfigurable intelligent surface (RIS) assisted wireless coverage extension: RIS orientation and location optimization," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 269–273, Jan. 2021.

[8] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Commun.*, vol. 29, no. 3, pp. 131–138, Jun. 2022.

[9] H. Huang, Y. Zhang, H. Zhang, C. Zhang, and Z. Han, "Illegal intelligent reflecting surface based active channel aging: When jammer can attack without power and CSI," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 11018–11022, Aug. 2023.

[10] H. Huang, Y. Zhang, H. Zhang, Y. Cai, A. L. Swindlehurst, and Z. Han, "Disco intelligent reflecting surfaces: Active channel aging for fully-passive jamming attacks," *IEEE Trans. Wireless Commun.*, in press, May 2023.

[11] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 24, no. 2, pp. 767–809, 2nd Quarter 2022.

[12] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming resilient communication using MIMO interference cancellation," *IEEE Trans. Inf. Forensic Secur.*, vol. 11, no. 7, pp. 1486–1499, Feb. 2016.

[13] K. T. Truong and R. W. Heath Jr., "Effects of channel aging in massive MIMO systems," *J. Commun. Netw-S. Kor.*, vol. 15, no. 4, pp. 338–351, Aug. 2013.

[14] E. Björnson, M. Bengtsson, and B. Ottersten, "Optimal multiuser transmit beamforming: A difficult problem with a simple solution structure," *IEEE Signal Process. Mag.*, vol. 31, no. 4, pp. 142–148, Jun. 2014.

[15] M. Sadek, A. Tarighat, and A. H. Sayed, "A leakage-based precoding scheme for downlink multi-user MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1711–1721, May 2007.

[16] T. X. Tran and K. C. Teh, "Spectral and energy efficiency analysis for SLNR precoding in massive MIMO systems with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 4017–4027, Jun. 2018.

[17] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.

[18] D. Shen, L. Dai, X. Su, and S. Suo, "Multi-beam design for near-field extremely large-scale RIS-aided wireless communications," *IEEE Trans. Green Commun. Netw.*, early access, Mar. 2023, doi: 10.1109/TGCN.2023.3259579.

[19] Further Advancements for E-UTRA Physical Layer Aspects (Release 9), document 3GPP TS 36.814, Mar. 2010.